VISA

January 19, 2007

Russell W. Schrader
Senior Vice President
Assistant General Counsel

By Electronic Delivery

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Identity Theft Task Force, P065410

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. in response to the Federal Identity Theft Task Force's ("Task Force") request for comment in connection with the production of a final strategic plan to combat identity theft. The Task Force, in working to produce a final strategic plan for the President, is considering, among other things, various ways to enhance data protection for sensitive consumer information maintained by the private sector. Visa appreciates the opportunity to comment on this important matter.

The Visa Payment System, of which Visa U.S.A.[1] is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud, for the benefit of Visa's member financial institutions and their hundreds of millions of cardholders.

In addition, Visa is committed to increasing the choice, convenience, acceptance and security of Visa payments for all stakeholders in the payment system—members, cardholders and merchants. Through its 13,420 member financial institutions, more than 488 million Visa-branded cards have been issued to cardholders in the United States.

Strategic Plan to Combat Identity Theft

Visa believes that the Task Force members have appropriately focused their work, in part, on keeping sensitive consumer data out of the hands of identity thieves through better data security practices and by educating consumers to protect themselves. As discussed more fully below, strong security measures and a consumer-focused approach to protecting sensitive information are inherent in the Visa system. For example, Visa has developed a number of

[1] Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

Visa U.S.A. Inc.
P.O. Box 194607
San Francisco, CA 94119-4607
U.S.A.
t 415 932 2178
f 415 932 2525

procedures and policies to help prevent the use of cardholder-related information for fraudulent purposes, such as the Cardholder Information Security Program ("CISP"). CISP applies to all entities that store, process, transmit or hold Visa cardholder data, including merchants, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers and the Internet.

CISP was developed to ensure that the customer information of Visa's members is protected and remains confidential. CISP includes provisions for monitoring compliance with CISP and sanctions for failure to comply. Visa was recently able to integrate CISP into the common set of data security requirements used by various credit card organizations without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, known as the Payment Card Industry Data Security Standard ("PCI Standard"), and believes that compliance with CISP and the PCI Standard will not only help protect cardholder-related information, but also will assist merchants in preventing data breaches. In addition to the strong security measures provided by CISP and the PCI Standard, Visa has established a zero liability standard for cardholders for unauthorized purchases involving Visa-branded payment cards. As a result, cardholders are not responsible for unauthorized purchases on their Visa cards.

Visa strongly urges the Task Force to recommend best practices, rather than regulatory or legislative proposals, to encourage the private sector to develop policies and procedures to prevent the misuse of consumer data that is not currently protected by federal law. If the Task Force believes that a legislative approach is appropriate, Visa recommends an approach that would impose a single, national risk-based standard for data security and for security breach notification. In this regard, it is important to note that existing federal law—namely, Title V of the Gramm-Leach-Bliley Act ("GBLA")—imposes strong data security and safeguarding requirements on financial institutions with respect to customer information. Specifically, the GLBA requires that financial institutions limit the disclosure of customer information and protect such information from unauthorized access and use. Moreover, the customer information security guidance, issued by the federal banking agencies pursuant to the GLBA, requires that banks notify their customers when there is a breach of security involving sensitive customer information. As a result, with respect to financial institutions subject to data security and/or security breach notification requirements under the GLBA, any new federal requirements should include a safe harbor for financial institutions that comply with the existing GLBA requirements by stating that compliance with such GLBA requirements would be deemed compliance with the new federal requirements.

Moreover, Visa believes that any Task Force recommendation for a legislative approach to security breach notification should recognize that the risks associated with each security breach will differ and, as a result, the appropriate response to each breach also will differ. As a result, any new federal requirements should adopt a risk-based approach that takes into account the likelihood that information has or will be used to harm consumers through identity theft or account fraud.

Visa Efforts to Combat Identity Theft

Visa, along with several financial services industry groups, has implemented industry guidance to prevent data breaches and to assist payment system participants (including financial institutions and merchants) in developing data security programs to better protect sensitive consumer information and to help financial institutions comply with federal and state laws.

New Account Data Compromise Recovery Process

For example, Visa implemented a new Account Data Compromise Recovery ("ADCR") process to resolve disputes related to account compromises that have been linked to magnetic stripe-read counterfeit fraud. The ADCR process, which went into effect on October 1, 2006, is designed to limit counterfeit fraud liability for acquirers and to allow for the partial recovery of some operating expenses for issuers.[2]

The ADCR process is used exclusively when magnetic stripe data is determined to be compromised. Once a merchant notifies its acquirer of an account compromise, the acquirer sends the stolen card account numbers directly to Visa's Compromised Account Management System ("CAMS"). Visa then validates that an account compromise has occurred and notifies issuers about the compromised accounts. Affected issuers can monitor or close the compromised accounts or block transactions that are attempted on such accounts.

If Visa determines that the validated account compromise meets the ADCR criteria, Visa calculates and advises the acquirer of its potential financial liability under the ADCR process. The potential financial liability of an acquirer is determined, in part, on a percentage of magnetic stripe-related counterfeit fraud estimated to occur during a maximum period of 13 months, which can be up to 12 months prior to and one month past the CAMS alert date. After Visa provides an estimate of the liability, the acquirer has 30 days to appeal the preliminary decision and to provide documentation to Visa.

At the end of the fraud-reporting period, Visa determines the actual financial liability to the acquirer based on the incremental level of counterfeit fraud—the level over the expected level of fraud—attributable to the exposure of the magnetic stripe data. Acquirers, at their discretion, determine when and how to notify a merchant about the merchant's estimated financial liability. Moreover, under the ADCR process, issuers can recover up to $1 per eligible account involved in the compromise to partially cover their fraud-related operating expenses, such as the costs of issuing replacement cards.

New PCI Data Security Standards

In September 2006, an updated version of the Payment Card Industry Data Security Standard ("PCI DSS") was issued. The PCI DSS consists of 12 requirements to protect

[2] The term "acquirers" refers to Visa member banks that acquire transactions from merchants that have accepted Visa payment cards in payment for transactions. In addition, the term "issuers" refers to Visa member banks that issue Visa payment cards to consumers.

cardholder data and sensitive authentication data, including requirements for security policies and procedures, network architecture and software design. These requirements, which apply to a wide range of entities that perform various roles in payment cards systems, are organized into six "control objectives": (1) build and maintain a secure network; (2) protect cardholder data; (3) maintain a vulnerability management program; (4) implement strong access control measures; (5) regularly test and monitor networks; and (6) maintain an information security policy. The PCI Security Standards Council has stated that the PCI DSS will be enhanced periodically, as needed, so that appropriate requirements are developed to mitigate payment security risks, while still fostering wide-scale adoption. Visa will continue to manage all enforcement and validation initiatives for Visa's CISP, which is consistent with the PCI DSS.

PCI Compliance Acceleration Program

To help accelerate compliance with PCI DSS and eliminate the storage of sensitive card data, Visa launched the Visa PCI Compliance Acceleration Program ("PCI CAP"). The program was developed with input from issuers and acquirers and will:

- Provide acquirers with up to $20 million in financial incentives for their merchants' validation of PCI compliance;
- Set an enforcement date for acquirers to validate PCI compliance; and
- Expand monetary fines for the storage of prohibited data and noncompliance with PCI DSS.

The program targets the largest merchants that each process more than 1 million Visa transactions per year and account for a large portion of Visa's U.S. transaction volume. By focusing attention on these merchants, Visa hopes to address a significant portion of the exposure to the payment system.

PCI Incentive Fund

The $20 million incentive fund will be payable to the acquiring financial institutions of the largest U.S. merchants that have already or will validate PCI compliance by August 31, 2007, and have not been involved in a data compromise. The program also will link the benefits of tiered interchange rates to PCI compliance, creating added compliance incentives for large merchants. Acquirers are encouraged to pass the incentive payments through to their merchants, but may use discretion in determining payout amounts and awarding payments. The funds also may be invested in related security compliance programs.

PCI Compliance Deadlines and Fines

In addition to offering financial incentives, PCI CAP will build on Visa's current compliance efforts by setting an enforcement date for acquirers to validate PCI compliance for the largest merchants and adding new financial fines for the storage of prohibited data. Fines will range from $5,000 to $25,000 per month and will be subject to escalation in the event material progress toward compliance is not made in a timely manner.

By combining financial incentives and fines, Visa expects the largest merchants—with the help of their acquirers—to accelerate their progress toward protecting both their payment systems and their customers against potential data compromises.

Once again, we appreciate the opportunity to comment on this important matter. If you have any questions concerning these comments or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me, at (415) 932-2178.

Sincerely,

Russell W. Schrader
Senior Vice President and
Assistant General Counsel